

Access tokens

After finding a service endpoint to interact with, it's time to request an access token. You can request one via your own Nuts node:

```
POST /internal/auth/v2/my_subject_identifier/request-service-access-token

{
  "authorization_server": "https://example.com/oauth2/other_subject_identifier",
  "scope": "coffee",
  "token_type": "Bearer",
  "credentials": [...]
}
```

- The `authorization_server` parameter is taken from the `authServerURL` registration parameter from the search result.
- The scope is determined by the use case.
- The `token_type` by default is `DPoP`, you can also choose for `Bearer`.
- You can pass additional holder credentials via `credentials`. This is a way to embed user identity tokens.

The `scope` is mapped by a policy file to a presentation definition. Policy files are provided by the use case. If your wallet contains the correct credentials according to the presentation definition, an access token will be given:

```
{
  "access_token": "ciOjSUzI1NiIslnR5cCl6lkp",
  "token_type": "Bearer",
  "expires_in": 3600,
}
```

The `access_token` can then be put in the HTTP Authorization header.

Revision #3

Created 23 September 2024 09:28:08 by Wout Slakhorst

Updated 23 September 2024 13:46:34 by Wout Slakhorst